UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/537,300	06/02/2005	Marc Joye	1032326-302	1466

21839 7590 09/02/2008
BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
09/02/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	10/537,300	JOYE, MARC	
	Examiner	Art Unit	
	LONGBIT CHAI	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 6/2/2006 but is a 371 case of PCT/FR03/03681 application filed 12/11/2003 and has a foreign priority application filed on 12/11/2002.

Response to Arguments

2. As per claim 1, Applicant remarks "There is no teaching or suggestion in Drexler of masking the number a because Drexler uses "a" known data M while Applicant uses secret data a" (Remarks: Page 6 / 1st Para). Examiner respectfully disagrees because Applicant's argument has no merit since the alleged limitation "using a secret data instead of a known data" has not been recited into the claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 2 and 5 – 8 are rejected under 35 U.S.C. 102(e) as being anticipated by Drexler et al. (U.S. Patent 2003/0079139).

As per claim 1, Drexler teaches a cryptographic method during which an integer division of the type q = a div b and/or a modular reduction of the type r = a mod b is performed, where q is a quotient, a is a number containing m bits, b is a number containing n bits, with n less than or equal to m and b_{n-1} is non-zero, b_{n-1} being the most significant bit of the number b (Drexler: Para [0004] and Para [0007]: a modular reduction used for a encryption / decryption process, n is indeed less than or equal to m), comprising the steps of:

masking the number a by a random number ρ before performing the integer division and/or the modular reduction (Drexler: Para [0020] Line 1 – 3 / Line 9 – 10: a random number r is first chosen for modular process (M mod n) by forming (r * n) which is added to the message M, where n is the modulus, as taught by Drexler – this is consistent with the disclosure of the specification of the instant application (SPEC: Page 10 Line 5), i.e., for modular process (a mod b) in order to mask the number a, b times the random number ρ is added to the number a, i.e. a <= a + (b * ρ));

generating encrypted or decrypted data in accordance with the results of the division and/or modular reduction (Drexler: Para [0005] Line 4).

As per claim 2, Drexler teaches in order to mask the number a, b times the random number ρ (a <= a + (b * ρ)) is added to the number a (Drexler: Para [0020] Line 1 – 3 / Line 9 – 10: a random number r is first chosen for modular process (M mod n) by forming (r * n) which is added to the message M, where n is the modulus, as taught by Drexler – this is consistent with the disclosure of the specification of the instant application (SPEC: Page 10 Line 5), i.e., for

modular process (a mod b) in order to mask the number a, b times the random number ρ is added to the number a, i.e. a <= a + (b * ρ)).

As per claim 5, Drexler teaches the random number ρ is modified at each implementation of the method (Drexler: Para [0017] Line 3: the random number r has a different value for each iteration).

As per claim 6, Drexler teaches the random number ρ is modified after a predetermined number of implementations of the method (Drexler: Para [0017] Line 3 – 4: the random number r has a different value for a predetermined number of iterations from 1 to k).

As per claim 7, Drexler teaches an electronic component (Drexler: Para [0009]) comprising means for implementing a method according to claim 1 (see claim 1 for the same rationale of rejection), said means comprising a plurality of registers for storing the numbers a and b (Drexler: Para [0011]: a semiconductor chip must have registers and memory to store and manipulate the input data such as memory registers and processing registers).

As per claim 8, Drexler teaches a chip card comprising a component according to claim 7 (Drexler: Para [0009]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art

> are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drexler et al. (U.S. Patent 2003/0079139), in view of Falk et al. (U.S. Patent 5,077,793).

As per claim 3, Drexler does not disclose expressly after having performed an integer division, the contribution made by the random number ρ is taken away from the result of the integer division.

Falk teaches having performed an integer division, the contribution made by the random number ρ is taken away from the result of the integer division (Falk : Column 6 Line 27 – 29, column 2 Line 38 – 43: the random number ρ is subtracted from the result of the integer division of encryption process).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Falk within the system of Drexler because (a) Drexler teaches preventing hidden channel attack during the cryptographic calculation process by imposing a random number r into the modulus operation of cryptographic process (Drexler : Para [0007] and Para [0020]) and (b) Falk teaches an effective encryption / decryption process within a modular residue number system that provides a minimum hardware to manipulate the random number for a high speed cryptographic calculation process (Falk : Abstract / Line 1 – 8 and Column 2 Line 21 – 24).

As per claim 4, Drexler as modified teaches the random number ρ is subtracted from the result of the integer division of encryption process (Falk : Column 6 Line 27 – 29, column 2 Line

38 – 43: the random number p is subtracted from the result of the integer division of encryption process).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai Ph.D.
Primary Patent Examiner
Art Unit 2131
08/27/2008